



BEST AVAILABLE COPY

WORLD INTELLECTUAL PROPERTY ORGANIZATION
ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE

34, chemin des Colombettes, Case postale 18, CH-1211 Genève 20 (Suisse)
Téléphone: (41 22) 338 91 11 - e-mail: wipo.mail @ wipo.int. - Fac-similé: (41 22) 733 54 28

PATENT COOPERATION TREATY (PCT)
TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

CERTIFIED COPY OF THE INTERNATIONAL APPLICATION AS FILED
AND OF ANY CORRECTIONS THERETO

COPIE CERTIFIÉE CONFORME DE LA DEMANDE INTERNATIONALE, TELLE QU'ELLE
A ÉTÉ DÉPOSÉE, AINSI QUE DE TOUTES CORRECTIONS Y RELATIVES

International Application No. }
Demande internationale n° }

PCT/IB 03 / 00343

International Filing Date }
Date du dépôt international }

03 FEBRUARY 2003
(03.02.03)

Geneva/Genève,

23 FEBRUARY 2004
(23.02.04)

International Bureau of the
World Intellectual Property Organization (WIPO)

Bureau International de l'Organisation Mondiale
de la Propriété Intellectuelle (OMPI)

CERTIFIED COPY OF
PRIORITY DOCUMENT



J.-L. Baron

Head, PCT Receiving Office Section
Chef de la section "office récepteur du PCT"

RT



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Lauri PAATERO Group No.:
Serial No.: 10/771,836
Filed: February 3, 2004 Examiner:
For: ARCHITECTURE FOR ENCRYPTED APPLICATION INSTALLATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy of the foreign application from which priority is claimed for this case, along with the certified translation of Tuulikki Tulivirta, Certified Translator:

Country : PCT
Application Number : PCT/IB03/00343
Filing Date : February 3, 2003

WARNING: "When a document that is required by statute to be certified must be filed, a copy, including a photocopy or facsimile transmission of the certification is not acceptable." 37 CFR 1.4(f) (emphasis added)

Francis J. Maguire

SIGNATURE OF ATTORNEY

Reg. No.: 31,391

Francis J. Maguire

Tel. No.: (203) 261-1234

Type or print name of attorney

Ware, Fressola, Van Der Sluys & Adolphson LLP
755 Main Street, P.O. Box 224
P.O. Address

Customer No.: 004955

Monroe, Connecticut 06468

NOTE: The claim to priority need be in no special form and may be made by the attorney or agent if the foreign application is referred to in the oath or declaration as required by § 1.63.

CERTIFICATE OF MAILING (37 CFR 1.10)

I hereby certify that this correspondence is, on the date shown below, being deposited with the United States Postal Service as first class mail in an envelope addressed to the: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: May 13, 2004

Deborah J. Clark

(Type or print name of person certifying)

Deborah J. Clark

(Signature of person mailing paper)

(Transmittal of Certified Copy [5-4])

PCT REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty

| | |
|--|---------------|
| For receiving Office use only | |
| PCT / IB 0 3 / 0 0 3 4 3 | |
| International Application No. | |
| 0 3 FEBRUARY 2003 | (0 3. 02. 03) |
| International Filing Date | |
| INTERNATIONAL BUREAU OF WIPO | |
| Name of Receiving Office and "PCT International Application" | |
| Applicant's or agent's file reference (if desired)(12 characters maximum) | PC-21002019 |

| | |
|---|---|
| Box No. I TITLE OF INVENTION | |
| ARCHITECTURE FOR ENCRYPTED APPLICATION INSTALLATION | |
| Box No. II APPLICANT <input type="checkbox"/> This person is also inventor. | |
| Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.) | Telephone No. |
| NOKIA CORPORATION | Facsimile No. |
| P.O. Box 226 | Teleprinter No. |
| FIN-00045 NOKIA GROUP | Applicant's registration No. with the Office |
| FINLAND | |
| State (that is, country) of nationality: FI | State (that is, country) of residence: FI |
| This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input checked="" type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box | |
| Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S) | |
| Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.) | This person is: |
| PAATERO, Lauri | <input type="checkbox"/> applicant only |
| Rikalantie 4 | <input checked="" type="checkbox"/> applicant and inventor |
| FIN-00970 Helsinki | <input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.) |
| FINLAND | Applicant's registration No. with the Office |
| State (that is, country) of nationality: FI | State (that is, country) of residence: FI |
| This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input checked="" type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box | |
| <input type="checkbox"/> Further applicants and/or (further) inventors are indicated on a continuation sheet | |
| Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE | |
| The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: | <input checked="" type="checkbox"/> agent <input type="checkbox"/> common representative |
| Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.) | Telephone No. |
| AWAPATENT AB | +46 8 440 95 00 |
| P.O. BOX 45086 | Facsimile No. |
| SE-104 30 STOCKHOLM | +46 8 440 95 50 |
| SWEDEN | Teleprinter No. |
| | Agent's registration No. with the Office |
| <input type="checkbox"/> Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent | |

Box No. V DESIGNATION OF STATES *Mark the applicable check-boxes below; at least one must be marked.*

The following designations are hereby made under Rule 4.9(a):

Regional Patent

- AP** **ARIPO Patent:** GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, MZ Mozambique, SD Sudan, SL Sierra Leone, SZ Swaziland, TZ United Republic of Tanzania, UG Uganda, ZM Zambia, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT *(if other kind of protection or treatment desired, specify on dotted line)*
- EA** **Eurasian Patent:** AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT
- EP** **European Patent:** AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, CZ Czech Republic, DE Germany, DK Denmark, EE Estonia, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, SI Slovenia, SK Slovakia, TR Turkey, and any other State which is a Contracting State of the European Patent Convention and of the PCT
- OA** **OAPI Patent:** BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GQ Equatorial Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)*

National Patent *(if other kind of protection or treatment desired, specify on dotted line):*

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> AE United Arab Emirates | <input checked="" type="checkbox"/> GM Gambia | <input checked="" type="checkbox"/> NZ New Zealand |
| <input checked="" type="checkbox"/> AG Antigua and Barbuda | <input checked="" type="checkbox"/> HR Croatia | <input checked="" type="checkbox"/> OM Oman |
| <input checked="" type="checkbox"/> AL Albania | <input checked="" type="checkbox"/> HU Hungary | <input checked="" type="checkbox"/> PH Philippines |
| <input checked="" type="checkbox"/> AM Armenia | <input checked="" type="checkbox"/> ID Indonesia | <input checked="" type="checkbox"/> PL Poland |
| <input checked="" type="checkbox"/> AT Austria | <input checked="" type="checkbox"/> IL Israel | <input checked="" type="checkbox"/> PT Portugal |
| <input checked="" type="checkbox"/> AU Australia | <input checked="" type="checkbox"/> IN India | <input checked="" type="checkbox"/> RO Romania |
| <input checked="" type="checkbox"/> AZ Azerbaijan | <input checked="" type="checkbox"/> IS Iceland | <input checked="" type="checkbox"/> RU Russian Federation |
| <input checked="" type="checkbox"/> BA Bosnia and Herzegovina | <input checked="" type="checkbox"/> JP Japan | |
| <input checked="" type="checkbox"/> BB Barbados | <input checked="" type="checkbox"/> KE Kenya | <input checked="" type="checkbox"/> SC Seychelles |
| <input checked="" type="checkbox"/> BG Bulgaria | <input checked="" type="checkbox"/> KG Kyrgyzstan | <input checked="" type="checkbox"/> SD Sudan |
| <input checked="" type="checkbox"/> BR Brazil | <input checked="" type="checkbox"/> KP Democratic People's Republic of Korea | <input checked="" type="checkbox"/> SE Sweden |
| <input checked="" type="checkbox"/> BY Belarus | <input checked="" type="checkbox"/> KR Republic of Korea | <input checked="" type="checkbox"/> SG Singapore |
| <input checked="" type="checkbox"/> BZ Belize | <input checked="" type="checkbox"/> KZ Kazakhstan | <input checked="" type="checkbox"/> SK Slovakia |
| <input checked="" type="checkbox"/> CA Canada | <input checked="" type="checkbox"/> LC Saint Lucia | <input checked="" type="checkbox"/> SL Sierra Leone |
| <input checked="" type="checkbox"/> CH & LI Switzerland and Liechtenstein | <input checked="" type="checkbox"/> LK Sri Lanka | <input checked="" type="checkbox"/> TJ Tajikistan |
| <input checked="" type="checkbox"/> CN China | <input checked="" type="checkbox"/> LR Liberia | <input checked="" type="checkbox"/> TM Turkmenistan |
| <input checked="" type="checkbox"/> CO Colombia | <input checked="" type="checkbox"/> LS Lesotho | <input checked="" type="checkbox"/> TN Tunisia |
| <input checked="" type="checkbox"/> CR Costa Rica | <input checked="" type="checkbox"/> LT Lithuania | <input checked="" type="checkbox"/> TR Turkey |
| <input checked="" type="checkbox"/> CU Cuba | <input checked="" type="checkbox"/> LU Luxembourg | <input checked="" type="checkbox"/> TT Trinidad and Tobago |
| <input checked="" type="checkbox"/> CZ Czech Republic +Utility Model | <input checked="" type="checkbox"/> LV Latvia | |
| <input checked="" type="checkbox"/> DE Germany +Utility Model | <input checked="" type="checkbox"/> MA Morocco | <input checked="" type="checkbox"/> TZ United Republic of Tanzania |
| <input checked="" type="checkbox"/> DK Denmark +Utility Model | <input checked="" type="checkbox"/> MD Republic of Moldova | <input checked="" type="checkbox"/> UA Ukraine |
| <input checked="" type="checkbox"/> DM Dominica | | <input checked="" type="checkbox"/> UG Uganda |
| <input checked="" type="checkbox"/> DZ Algeria | <input checked="" type="checkbox"/> MG Madagascar | <input checked="" type="checkbox"/> US United States of America |
| <input checked="" type="checkbox"/> EC Ecuador | <input checked="" type="checkbox"/> MK The former Yugoslav Republic of Macedonia | |
| <input checked="" type="checkbox"/> EE Estonia +Utility Model | <input checked="" type="checkbox"/> MN Mongolia | <input checked="" type="checkbox"/> UZ Uzbekistan |
| <input checked="" type="checkbox"/> ES Spain | <input checked="" type="checkbox"/> MW Malawi | <input checked="" type="checkbox"/> VC Saint Vincent and the Grenadines |
| <input checked="" type="checkbox"/> FI Finland +Utility Model | <input checked="" type="checkbox"/> MX Mexico | <input checked="" type="checkbox"/> VN Viet Nam |
| <input checked="" type="checkbox"/> GB United Kingdom | <input checked="" type="checkbox"/> MZ Mozambique | <input checked="" type="checkbox"/> YU Yugoslavia |
| <input checked="" type="checkbox"/> GD Grenada | <input checked="" type="checkbox"/> NO Norway | <input checked="" type="checkbox"/> ZA South Africa |
| <input checked="" type="checkbox"/> GE Georgia | | <input checked="" type="checkbox"/> ZM Zambia |
| <input checked="" type="checkbox"/> GH Ghana | | <input checked="" type="checkbox"/> ZW Zimbabwe |

Check-boxes below reserved for designating States which have become party to the PCT after issuance of this sheet:

- | | | |
|--------------------------------|--------------------------------|--------------------------------|
| <input type="checkbox"/> _____ | <input type="checkbox"/> _____ | <input type="checkbox"/> _____ |
| <input type="checkbox"/> _____ | <input type="checkbox"/> _____ | <input type="checkbox"/> _____ |

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. *(Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)*

| Box No. VI PRIORITY CLAIM | | | | |
|---|----------------------------------|----------------------------------|---|--|
| The priority of the following earlier application(s) is hereby claimed: | | | | |
| Filing date of earlier application (day/month/year) | Number of earlier application | Where earlier application is: | | |
| | | national application: country | regional application:* regional Office | international application: receiving Office |
| item (1) -- | | | | |
| item (2) | | | | |
| item (3) | | | | |
| item (4) | | | | |
| item (5) | | | | |

Further priority claims are indicated in the Supplemental Box.

The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) (*only if the earlier application was filed with the Office which for the purposes of this international application is the receiving Office*) identified above as:

- all items
 item (1)
 item (2)
 item (3)
 item (4)
 item (5)
 other, see Supplemental Box

* Where the earlier application is an ARIPO application, indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed (Rule 4.10(b)(ii)):

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) (*if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used*):

ISA / EP

Request to use results of earlier search; reference to that search (*if an earlier search has been carried out by or requested from the International Searching Authority*):

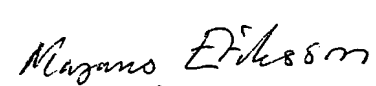
| Date (day/month/year) | Number | Country (or regional Office) |
|-----------------------|--------|------------------------------|
| -- | | |

Box No. VIII DECLARATIONS

The following **declarations** are contained in Boxes Nos. VIII (i) to (v) (*mark the applicable check-boxes below and indicate in the right column the number of each type of declaration*):

| | Number of declarations |
|--|------------------------|
| <input type="checkbox"/> Box No. VIII (i) Declaration as to the identity of the inventor | : |
| <input type="checkbox"/> Box No. VIII (ii) Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent | : |
| <input type="checkbox"/> Box No. VIII (iii) Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application | : |
| <input type="checkbox"/> Box No. VIII (iv) Declaration of inventorship (only for the purposes of the designation of the United States of America) | : |
| <input type="checkbox"/> Box No. VIII (v) Declaration as to non-prejudicial disclosures or exceptions to lack of novelty | : |

| Box No. IX CHECK LIST; LANGUAGE OF FILING | |
|--|---|
| <p>This international application contains:</p> <p>(a) in paper form, the following number of sheets:</p> <p>request (including declaration sheets) : 4</p> <p>description (excluding sequence listings and/or tables related thereto) : 12</p> <p>claims : 4</p> <p>abstract : 1</p> <p>drawings : 3</p> <p>Sub-total number of sheets : 24</p> <p>sequence listings : tables related thereto :</p> <p><i>(for both, actual number of sheets if filed in paper form, whether or not also filed in computer readable form; see (c) below)</i></p> <p>Total number of sheets : 24</p> <p>(b) <input type="checkbox"/> only in computer readable form (Section 801(a)(i))</p> <p>(i) <input type="checkbox"/> sequence listings</p> <p>(ii) <input type="checkbox"/> tables related thereto</p> <p>(c) <input type="checkbox"/> also in computer readable form (Section 801(a)(ii))</p> <p>(i) <input type="checkbox"/> sequence listings</p> <p>(ii) <input type="checkbox"/> tables related thereto</p> <p>Type and number of carriers (diskette, CD-ROM, CD-R or other) on which are contained the</p> <p><input type="checkbox"/> sequence listings:</p> <p><input type="checkbox"/> tables related thereto:</p> <p><i>(additional copies to be indicated under items 9(ii) and/or 10(ii), in right column)</i></p> | <p>This international application is accompanied by the following item(s) (mark the applicable check-boxes below and indicate in right column the number of each item):</p> <p>1. <input type="checkbox"/> fee calculation sheet : 2. <input type="checkbox"/> original separate power of attorney : 3. <input type="checkbox"/> original general power of attorney : 4. <input checked="" type="checkbox"/> copy of general power of attorney; reference number, if any: <u>GPA 02/0021</u> : 1</p> <p>5. <input type="checkbox"/> statement explaining lack of signature : 6. <input type="checkbox"/> priority document(s) identified in Box No. VI as item(s):</p> <p>7. <input type="checkbox"/> translation of international application into (language):</p> <p>8. <input type="checkbox"/> separate indications concerning deposited microorganism or other biological material : 9. <input type="checkbox"/> sequence listing in computer readable form (indicate type and number of carriers)</p> <p>(i) <input type="checkbox"/> copy submitted for the purposes of international search under Rule 13ter only (and not as part of the international application) : (ii) <input type="checkbox"/> (only where check-box (b)(i) or (c)(i) is marked in left column) additional copies including, where applicable, the copy for the purposes of international search under Rule 13ter : (iii) <input type="checkbox"/> together with relevant statement as to the identity of the copy or copies with the sequence listings mentioned in left column: :</p> <p>10. <input type="checkbox"/> tables in computer readable form related to sequence listings (indicate type and number of carriers)</p> <p>(i) <input type="checkbox"/> copy submitted for the purposes of international search under Section 802(b-quater) only (and not as part of the international application) : (ii) <input type="checkbox"/> (only where check-box (b)(ii) or (c)(ii) is marked in left column) additional copies including, where applicable, the copy for the purposes of international search under Section 802(b-quater) : (iii) <input type="checkbox"/> together with relevant statement as to the identity of the copy or copies with the tables mentioned in left column: :</p> <p>11. <input type="checkbox"/> other (specify):</p> |
| <p>Figure of the drawings which should accompany the abstract: 1</p> | <p>Language of filing of the international application: English</p> |

| Box No. X SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE |
|--|
| <p><i>Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).</i></p> <p>3 February 2003</p> <p style="text-align: center;"></p> <p>Magnus Eriksson Authorised representative</p> |

| For receiving Office use only | |
|--|--|
| <p>1. Date of actual receipt of the purported international application: 03 FEBRUARY 2003</p> <p>3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:</p> <p>4. Date of timely receipt of the required corrections under PCT Article 11(2):</p> <p>5. International Searching Authority (if two or more are competent): ISA/ EP</p> | <p>2. Drawings:</p> <p><input type="checkbox"/> received:</p> <p><input type="checkbox"/> not received:</p> <p>6. <input checked="" type="checkbox"/> Transmittal of search copy delayed until search fee is paid.</p> |

| For International Bureau use only |
|--|
| <p>Date of receipt of the record copy by the International Bureau:</p> |

ARCHITECTURE FOR ENCRYPTED APPLICATION INSTALLATIONTechnical Field of the Invention

The present invention relates to methods for providing, and systems arranged to provide, an application to be executed on a device, the device being
5 arranged with a secure environment to which access is strictly controlled by a device processor.

Background Art

Various electronic devices, such as mobile tele-
10 communication terminals, portable computers and PDAs require access to security related components such as application programs, cryptographical keys, cryptographical key data material, intermediate cryptographical
15 calculation results, passwords, authentication of externally downloaded data etc. It is often necessary that these components, and the processing of them, is kept secret within the electronic device. Ideally, they shall be known by as few people as possible. This is due to the fact that a device, for example a mobile terminal, could
20 possibly be tampered with if these components are known. Access to these types of components might aid an attacker with the malicious intent to manipulate a terminal.

Therefore, a secure execution environment is introduced in which environment a processor within the elec-
25 tronic device is able to access the security related components. Access to the secure execution environment, processing in it and exit from it should be carefully controlled. Prior art hardware comprising this secure environment is often enclosed within a tamper resistant
30 packaging. It should not be possible to probe or perform measurements and tests on this type of hardware which could result in the revealing of security related components and the processing of them.

Providers of application programs encrypt the programs so as to create tamper resistant software. Only when the application program code is executed in a secure environment, the code is decrypted and managed as plain
5 text.

David Lie et al, "Architectural Support for Copy and Tamper Resistant Software", published in Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS-
10 IX), November, 2000, Pp 169-177 discloses a system called XOM, eXecute Only Memory. Every XOM processor has a public/private key pair, and the private key is kept in hardware and known only to the processor, not to the owner of the processor or anyone else. When XOM software
15 is purchased, the software undergoes encryption, by means of this public/private key pair. The executable code is decrypted by the processor just before execution and the plaintext code never leaves the processor chip. A problem with this type of architecture is that the application
20 providers have very limited possibilities to define the way the application is handled during application installation.

Summary of the Invention

25 It is an object of the present invention to mitigate the above stated problem, as well as providing a system which facilitates modifications in key management and encryption systems.

This object is achieved by methods for providing an
30 application to be executed on a device, the device being arranged with a secure environment to which access is strictly controlled by a device processor, according to claim 1 and claim 2 and systems arranged to provide an application to be executed on a device, the device being
35 arranged with a secure environment to which access is strictly controlled by a device processor, according to claim 8 and claim 9.

According to a first aspect of the invention, a method is provided in which the device is provided with an encrypted application and, via a secure channel into the secure environment, a first key for decrypting the encrypted application. The encrypted application is decrypted in the secure environment by means of the first key. Further, the application is re-encrypted in the secure environment by means of a second key and the re-encrypted application is then stored outside the secure environment.

According to a second aspect of the invention, a method is provided in which the device is provided with an encrypted application and, via a secure channel into the secure environment, a first key for decrypting the encrypted application. Further, the first key is encrypted in the secure environment by means of a second key and the encrypted key is then stored outside the secure environment.

According to a third aspect of the invention, a system is provided, wherein means is arranged to provide the device with an encrypted application and, via a secure channel into the secure environment, a first key for decrypting the encrypted application. Means is arranged to decrypt the encrypted application in the secure environment using the first key. Further, means is arranged to re-encrypt the application in the secure environment using a second key and the re-encrypted application is then stored outside the secure environment.

According to a fourth aspect of the invention, a system is provided, wherein means is arranged to provide the device with an encrypted application and, via a secure channel into the secure environment, a first key for decrypting the encrypted application.. Further, the means is arranged to encrypt the first key in the secure environment using a second key and the encrypted key is then stored outside the secure environment.

The invention is based on the idea that an application is downloaded to a device which is arranged to execute the application. The application is divided into an installation part that establishes proper set up of the application and a protected part which is to be executed in the secure environment. The installation part produces an encrypted application, i.e. the protected part, and keys for decrypting it. The installation part might be encrypted using some arrangement known in the prior art. In this phase of the application installation, the downloaded data is held in a part of the device having milder security requirements than the secure environment. This part is hereinafter referred to as the unsecure environment. When the application is downloaded into the device, the installation part establishes a secure channel with a server that, on the secure channel, provides a first key into the secure environment of the device, with which first key it is possible to decrypt the encrypted application. It might be necessary for the device to authenticate itself in order to receive the first key. When the encrypted application is to be executed, it is loaded into the secure environment and decrypted by the first key. The application is now in plain text and can be executed. When there is no desire to execute the application, it is re-encrypted by means of a second key and stored outside the secure environment, i.e. in the unsecure environment. An advantage with this inventive idea is that the application provider has the freedom to control the decryption of the application software. Since it is performed in the secure environment, the owner of the device, the device being e.g. a mobile phone, is unable to access the application and thereby copy, read or manipulate it. Moreover, the application provider handles the installation of the encrypted application and the key for decrypting the application, and is thus given the possibility to handle the encryption/decryption schemes and the key management.

The only part that has to stay fixed is the loading part of the application, i.e. the part of the application which loads data into the secure environment and handles the decryption of the encrypted application. A further
5 advantage is that the application can be re-encrypted in the secure environment by a second key and stored outside the secure environment. When the application is not executed, it is not stored in the secure environment. Secure environment memory is relatively expensive
10 compared to unsecure environment memory located. As soon as the application is to be executed again, the re-encrypted application is loaded into the secure environment and decrypted by means of the second key.

According to an embodiment of the invention, the
15 first key is encrypted in the secure environment by means of the second key. The encrypted first key is then stored outside the secure environment. This embodiment has the advantage that the first key can be used in future downloads of applications. All that has to be done is to
20 encrypt the first key in the secure environment with the second key and store the encrypted first key outside the secure environment. The first key can then be used to decrypt a downloaded encrypted application in the secure environment. This is done by loading the encrypted first
25 key into the secure environment and decrypting it with the second key. This means that the installation step, including setting up a secure channel, of the first key need not be employed. This is particularly useful in production and/or in the development phase, wherein a
30 large number of applications might be downloaded to the device in a rather short time.

According to another embodiment of the present invention, the second key is symmetric and derived from the application in such a way that the second key is
35 comprised in the application itself and extracted when the application is loaded into the secure environment and decrypted by the first key. This has the advantage that

the application provider is given the freedom to decide which key to be used in the encryption/decryption relating to the second key. The second key management can then be controlled by the application provider. The fact
5 that the second key is symmetric implies that the encryption/decryption using the second key will be less computationally demanding compared to if it had been asymmetric.

According to yet another embodiment of the present
10 invention, the second key is symmetric and derived from the application using an application seed. By using an application seed in the form of, for example, an application serial number, it is possible to create the second key. The serial number is encrypted by means of an appropriate algorithm in the secure environment using a device
15 generated static key, and this operation creates the symmetric second key. This embodiment has the advantage that the second key must not be distributed, but it can be generated rather easy in the secure environment.

20 Further features of, and advantages with, the present invention will become apparent when studying the appended claims and the following description. Those skilled in the art realize that different features of the present invention can be combined to create embodiments
25 other than those described in the following. Many different alterations, modifications and combinations will become apparent for those skilled in the art. The described embodiments are therefore not intended to limit the scope of the invention, as defined by the appended
30 claims.

Brief Description of the Drawings

The present invention will be described in greater detail with reference to the following drawings, wherein:

35 Fig. 1 shows a block scheme of a device architecture for providing data security in which device the present invention advantageously can be applied;

Fig. 2 shows a block scheme of how the encrypted application is loaded into the secure environment and decrypted into plain text, i.e. into executable form, according to an embodiment of the invention; and

5 Fig. 3 shows how the symmetric second key is derived from the application according to an embodiment of the invention.

Description of Preferred Embodiments of the Invention

10 A device architecture for providing data security is shown in Fig. 1. Such a system is further disclosed in the Applicant's international patent applications PCT/IB02/03216, which application is incorporated herein by reference. The device is implemented in the form of an
15 ASIC (Application Specific Integrated Circuit) 101. The processing part of the architecture contains a CPU 103 and a digital signal processor (DSP) 102.

The secure environment 104 comprises a ROM 105 from which the ASIC 101 is booted. This ROM 105 contains boot
20 application software and an operating system. Certain application programs residing in the secure environment 104 has precedence over other application programs. In a mobile telecommunication terminal, in which the ASIC 101 can be arranged, a boot software should exist, which
25 software includes the main functionality of the terminal. It is not possible to boot the terminal to normal operating mode without this software. This has the advantage that by controlling this boot software, it is also possible to control the initial activation of each
30 terminal.

The secure environment 104 also comprises RAM 106 for storage of data and applications. The RAM 106 preferably stores so called protected applications, which are smaller size applications for performing security
35 critical operations inside the secure environment 104. Normally, the way to employ protected applications is to let "normal" applications request services from a certain

protected application. New protected applications can be downloaded into the secure environment 104 at any time, which would not be the case if they would reside in ROM. Secure environment 104 software controls the download and execution of protected applications. Only signed protected applications are allowed to run. The protected applications can access any resources in the secure environment 104 and they can also communicate with normal applications for the provision of security services.

10 In the secure environment 104, a fuse memory 107 is comprised containing a unique random number that is generated and programmed into the ASIC 101 during manufacturing. This random number is used as the identity of a specific ASIC 101 and is further employed to derive keys
15 for cryptographic operations. The architecture further comprises a standard bridge circuit 109 for limitation of data visibility on the bus 108. The architecture should be enclosed within a tamper resistant packaging. It should not be possible to probe or perform measurements
20 and tests on this type of hardware which could result in the revealing of security related components and the processing of them. The DSP 102 has access to other peripherals 110 such as a direct memory access (DMA) unit, RAMs, flash memories and additional processors can
25 be provided outside the ASIC 101.

By providing the above described architecture in which the CPU 103 is operable in two different modes, one secure operating mode and one unsecure operating mode, the CPU 103 of the device 101 can be enabled to execute
30 non-verified software downloaded into the device 101. This is due to the fact that only verified software has access to the secure environment 104. This allows testing, debugging and servicing of the mobile telecommunication terminal and its software without risking
35 that a third party is given access to information which makes it possible to manipulate the security related

components of the device 101 so as to affect the security functions when in the secure environment 104.

In the secure mode, the processor 103 has access to security related data located within the secure environment 104. The security data include cryptographical keys and algorithms, software for booting the circuitry, secret data such as random numbers used as cryptographical key material, application programs etc. The device 101 can advantageously be used in mobile telecommunication terminals, but also in other electronic devices such as computers, PDAs or other devices with need for data protection. The access to these security data and the processing of them need to be restricted, since an intruder with access to security data could manipulate the terminal. When testing and/or debugging the terminal, access to security information is not allowed. For this reason, the processor 103 is placed in the unsecure operating mode, in which mode it is no longer given access to the protected data within the secure environment 104.

Fig. 2 shows a block scheme of how the encrypted application is loaded into the secure environment and decrypted into plain text, i.e. into executable form. First, an application 202 is loaded 211 into a device 201 which is arranged to execute the application 202. The application 202 is divided into an installation part 203 that establishes proper set up of the application 202 and a protected part 204 which is to be executed in the secure environment 205. The installation part 203 produces an encrypted application, i.e. the protected part 204, and keys for decrypting it. The installation part 203 is not encrypted. At this stage of the installation, the application 202 is held in the unsecure environment 206. When the application 202 is loaded into the device 201, the installation part 203 establishes a secure channel 207 with a server 208 that, on the secure channel 207, provides a first key into the secure

environment 205 of the device 201, with which first key it is possible to decrypt the encrypted application 204. The secure channel 207 can be created in a number of different ways. It is, for example, possible to encrypt
5 the first key at the server 208 by using the public key of the device 201. It is decrypted with the private key of the device 201 in the secure environment 205. Thus, a secure channel is provided. It is also possible to use the SSL protocol to transfer the first key into the
10 secure environment 205. The key issue is that the first key is encrypted in such a way that a third party is unable to eavesdrop on the channel 207 and catch a plain text version of the first key. When the encrypted application 204 is to be executed, it is loaded into the
15 secure environment 205 and decrypted by the first key. The protected application is now in plain text 209 and can be executed. When there is no desire to execute the plain text application 209 in the secure environment 205, it is re-encrypted by means of a second key and stored in
20 the unsecure environment 206.

The second key is symmetric and can be derived from the application in different ways. Referring to Fig. 3, which shows the application 301 that is downloaded to the device 305, including the installation part 302 and the
25 protected application part (also referred to herein as the encrypted application) 303. The second key is denoted by 304 and is attached to the application code itself. Note that the second key forms part of the protected application 303 and is consequently also encrypted by
30 means of the first key. The second key is extracted when the protected application 303 is loaded into the secure environment 306 and decrypted by the first key. The application 307 as well as the second key 308 is then in plain text. The second key can also be derived from the
35 application using an application seed. By using an application seed in the form of, for example, an application serial number, it is possible to create the second

key. The serial number is encrypted by means of an appropriate algorithm in the secure environment using a device generated static key, and this operation creates the symmetric second key. This operation is called
5 diversification.

Referring again to Fig. 2, according to an embodiment of the invention, the first key is encrypted in the secure environment 205 by means of the second key. The encrypted first key is then stored in the unsecure
10 environment 206. This embodiment has the advantage that the first key can be used in future downloads of applications 202. All that has to be done is to encrypt the first key in the secure environment 205 with the second key and store the encrypted first key in the unsecure
15 environment 206. The first key can then be used to decrypt a downloaded encrypted application 204 in the secure environment 205. This is done by loading the encrypted first key into the secure environment 205 and decrypting it with the second key. The protected applica-
20 tion 204 is then decrypted with the first key. This means that the installation step, including setting up a secure channel 207, of the first key need not be employed. This is particularly useful in production and/or in the development phase, wherein a large number of applications
25 202 might be downloaded to the device 201 in a rather short time. In production and/or in the development phase, it is also advantageous to transfer multiple keys successively on the secure channel into the secure environment, since each key later can be used to decrypt
30 an encrypted application that corresponds to that key the in the secure environment.

It should be noted that the above mentioned embodiments exemplify the invention, and that those skilled in the art will be able to design many alternative embodi-
35 ments without departing from the scope of the appended claims. The word "comprising" does not exclude the presence of elements or ~~steps~~ other than those listed in

a claim. The word "a" or "an" preceding an element does not exclude the presence of a plurality of such elements. In the device claims enumerating several means, several of these means can be embodied by one and the same item
5 of hardware.

CLAIMS

1. A method for providing an application to be executed on a device, the device being arranged with a secure environment to which access is strictly controlled
5 by a device processor, the method comprising:

providing the device (201) with an encrypted application (204);

providing, via a secure channel (207) into the secure environment (205), the device (201) with a first
10 key for decrypting said encrypted application (204);

decrypting, in the secure environment (205), said encrypted application (204) by means of said first key;

re-encrypting, in said secure environment, the application (209) by means of a second key; and

15 storing, outside said secure environment, the re-encrypted application.

2. A method for providing an application to be executed on a device, the device being arranged with a
20 secure environment to which access is strictly controlled by a device processor, the method comprising:

providing the device (201) with an encrypted application (204);

providing, via a secure channel (207) into the secure environment (205), the device (201) with a first
25 key for decrypting said encrypted application (204);

encrypting, in said secure environment (205), said first key by means of a second key; and

30 storing, outside said secure environment (205), the encrypted first key.

3. The method according to claim 1, the method comprising:

35 encrypting, in said secure environment (205), said first key by means of the second key; and

storing, outside said secure environment (205), the re-encrypted first key.

4. The method according to claim 1 or 2, wherein said second key is symmetric and can be derived from the application (202).

5 5. The method according to claim 4, wherein said second key is comprised in the application (202) itself.

6. The method according to claim 4, wherein said second key is generated in the secure environment (205) using an application seed.

7. The method according to any of the previous claims, wherein multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

8. A system arranged to provide an application to be executed on a device, the device being arranged with a secure environment to which access is controlled by a device processor, the system comprising:

 means for providing the device (201) with an encrypted application (204);

 means for providing, via a secure channel (207) into the secure environment (205), the device (201) with a first key for decrypting said encrypted application (204);

 means for decrypting, in the secure environment (205), said encrypted application (204) by means of said first key;

 means for re-encrypting, in said secure environment, the application (209) by means of a second key; and

 means for storing, outside said secure environment, the re-encrypted application.

9. A system arranged to provide an application to be executed on a device, the device being arranged with a secure environment to which access is controlled by a device processor, the system comprising:

5 means for providing the device (201) with an encrypted application (204);

means for providing, via a secure channel (207) into the secure environment (205), the device (201) with a first key for decrypting said encrypted application
10 (204);

means for encrypting, in said secure environment (205), said first key by means of a second key; and

means for storing, outside said secure environment (205), the encrypted first key.

15

10. The system according to claim 8, the system comprising:

means for encrypting, in said secure environment (205), said first key by means of the second key; and

20 means for storing, outside said secure environment (205), the encrypted first key.

11. The system according to claim 8 or 9, wherein said second key is symmetric and can be derived from the
25 application (202).

12. The system according to claim 11, wherein said second key is comprised in the application (202) itself.

30 13. The system according to claim 11, wherein said second key is generated in the secure environment (205) using an application seed.

35 14. The system according to any of the claims 8-13, wherein the system is arranged such that multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to

decrypt a corresponding encrypted application in the secure environment.

ABSTRACT

The present invention relates to methods to control, and systems arranged to control, the decryption of a provided encrypted application in a device executing the application, the device being arranged with a secure environment to which access is strictly controlled by a device processor. The invention is based on the idea that the application is divided into an installation part that establishes proper set up of the application and a protected part which is to be executed in the secure environment. An advantage with the invention is that the application provider has the freedom to control the decryption of the application software. Since it is performed in the secure environment, the owner of the device, is unable to access the application and thereby copy, read or manipulate it. Moreover, the application provider handles the installation of the encrypted application and the key for decrypting the application, and is thus given the possibility to handle the encryption/decryption schemes and the key management.

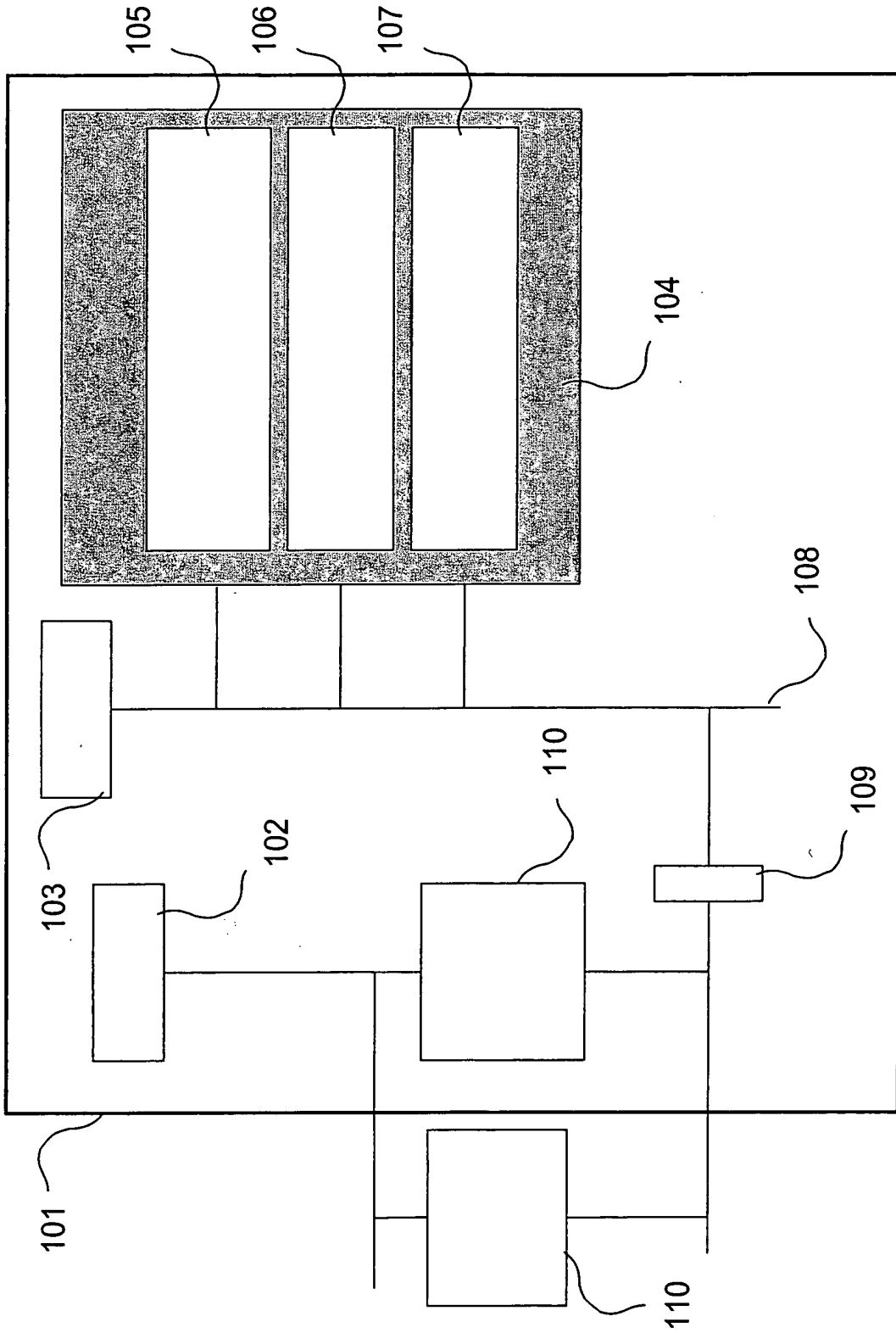


Fig. 1

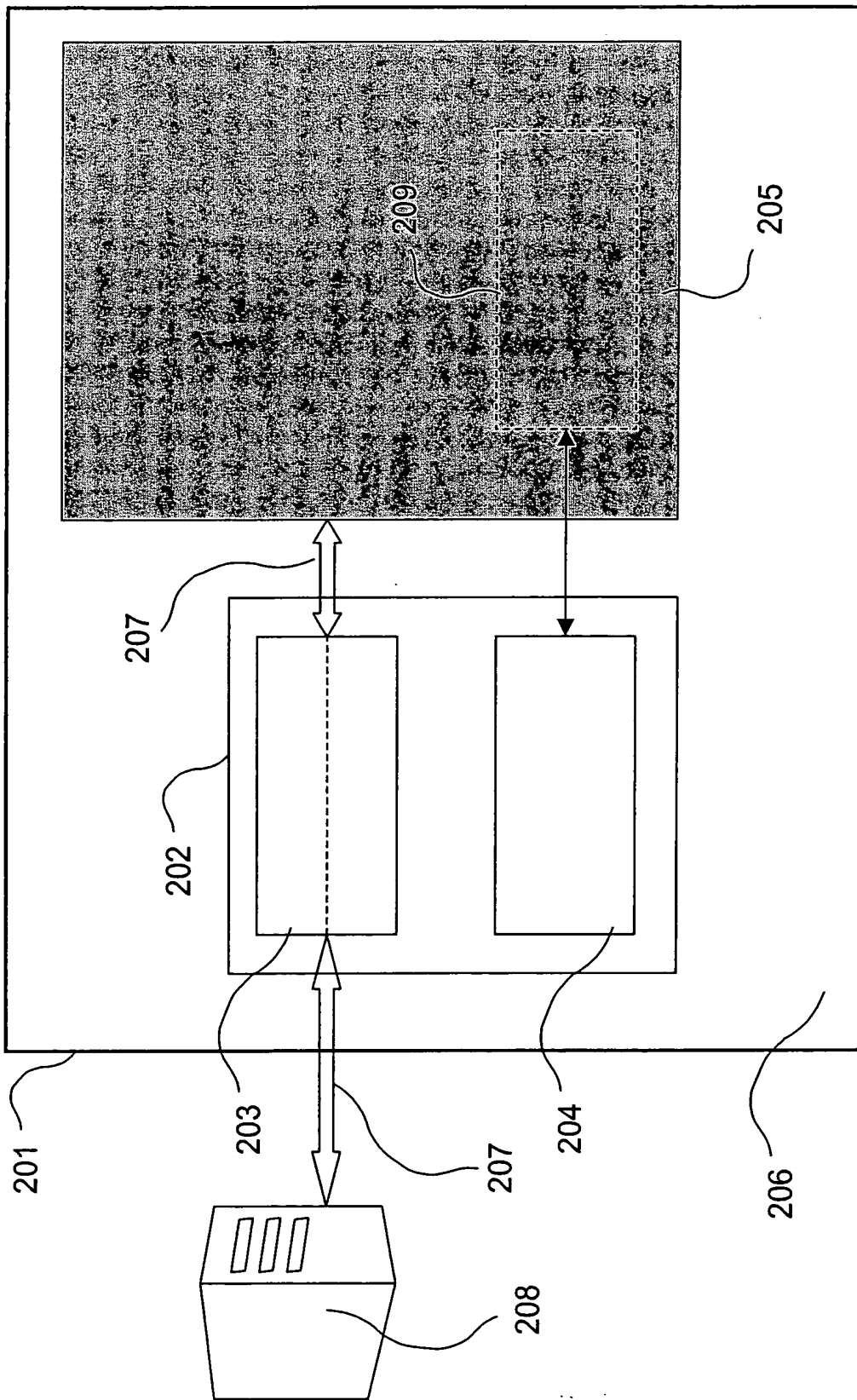


Fig. 2

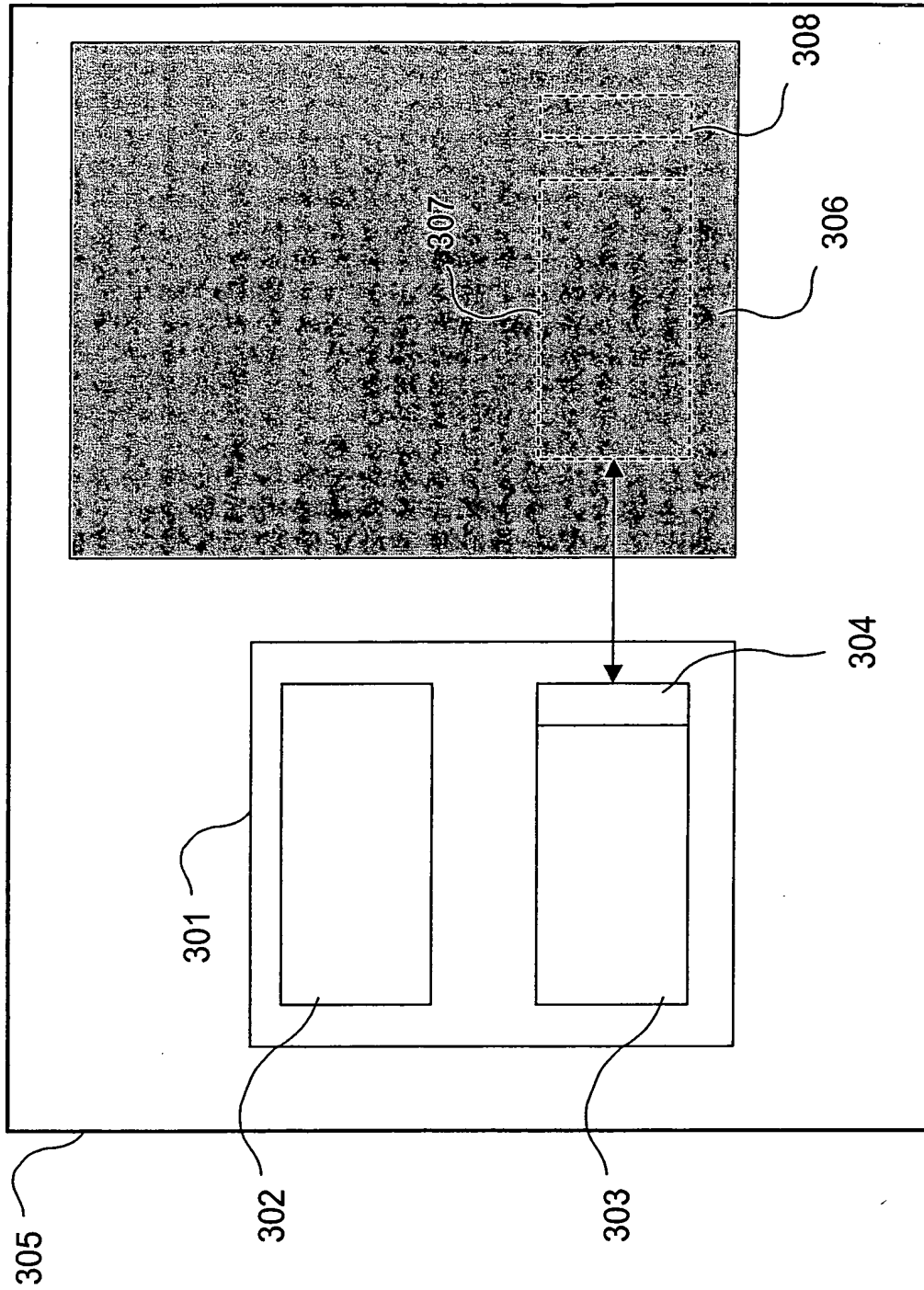


Fig. 3